REMARKS

This Amendment responds to the office action dated October 15, 2007. Reconsideration is respectfully requested.

A) Rejections under 35 U.S.C. § 102

Claims 1-45 were rejected under 35 U.S.C. § 102(e) as being anticipated by Schneier (U.S. Pat. 5,956,404). In the prior office action, however, the Examiner indicated that "applicant's arguments with respect to Schneier's failure to specifically disclose the two part use of an ephemeral key pair are in fact persuasive." The Examiner nevertheless maintained the 102 rejections due to the section 112 issues discussed below. Applicant maintains that in view of the claim amendments and remarks set forth herein, the section 112 rejections have now been overcome, and thus the 102 rejection over Schneier should be withdrawn.

C) Rejections under 35 U.S.C. § 112

In the Office Action, the Examiner continues to reject the claims as being indefinite and not enabled under 35 U.S.C. § 112. Specifically, at page 3 of the Office Action, the Examiner states that the 112 rejections are maintained "until they [the claims] are amended to clarify the extent and duration of the ephemeral key pair. . ." and further states that "[i]f it it's the Applicant's intent to provide for an ephemeral key pair to be used for a single message transaction, that transaction including the encrypting of a plaintext message and the generation of a digital signature, all using the same ephemeral key pair, the Examiner requests that the Applicant make the amendments necessary." (Office Action at 3)

Applicant respectfully submits that the rejected claims are definite and enalbed under 35 U.S.C. § 112 and that the rejection should be withdrawn; however, in order to expedite issuance in this matter, the independent claims have now been amended to further clarify the extent and

duration of use of the claimed "ephemeral key pair," per the Examiner's suggestion. Specifically, the claims have been amended, consistent with the specification and figures, to state that "*for each message transaction*" in a plurality of message transactions between a sender and a receiver, a plaintext message is encrypted using an ephemeral key pair, and a digital signature is generated for the encrypted message using the same ephemeral key pair produced in the encryption step. In addition, the claims have been amended to specify that "*the ephemeral key pair used in the encrypting and generating steps is used for a single message transaction in the plurality of message transactions between the sender and the receiver.*" Thus, the claims have been clarified to specify the extent and duration of the ephemeral key pair by limiting its use to a single message transaction in a plurality of transactions between a sender and a receiver. Moreover, the claims now specify the Applicant's intent to provide for an ephemeral key pair to be used for a single message transaction, that transaction including the encrypting of a plaintext message and the generation of a digital signature, all using the same ephemeral key pair, as suggested by the Examiner in the Office Action. Thus, the section 112 indefiniteness rejection should be withdrawn.

The dual use of such a per-message ephemeral key pair is clearly supported by the specification, and one of skill in the art would be enabled to practice the claimed invention in view of at least the following explicit support thereof. Page 4, lines 6-9 of the specification, for example, state "in the present invention, there is provided an improved encryption and digital signature scheme ***that reuses an ephemeral key pair from the encryption process in the signature process***. Advantageously, the reuse of the ephemeral key allows the digital signature to be reduced in byte size." (emphasis supplied) In addition, page 5, lines 7-9 of the

specification state "the improved digital signature scheme uses the value of *x*, an encryption ephemeral key, for the value of *z*, a signature ephemeral key, instead of generating a random value for *z*, as in the prior art." Moreover, the problems in the prior art method of generating two separate ephemeral key pairs, one for the encryption phase and a second for the digital signature phase, are highlighted at page 9, lines 5-9 of the specification as follows "[F]irstly, computational resources and time consumed where Z is calculated with large bit numbers. Secondly, the byte-size overhead associated with the public-key transmitted information is undesirably large for bandwidth sensitive devices such as wireless communication devices."

Figure 4 of the present application, set forth below, clearly demonstrates the dual-use sharing of the temporary ephemeral key pair in the message encryption and digital signature phases of a public key encryption process on a per message basis. In Figure 4, the encryption ephemeral key pair (x, X) is generated in the encryption phase 16, which generates a ciphertext message using this temporary key pair. Then, in the digital signature phase 32, instead of generating another temporary key pair for the digital signature process, the ephemeral key pair (x, X) from the encryption phase is re-used in the digital signature phase by setting z to x and Z to X.

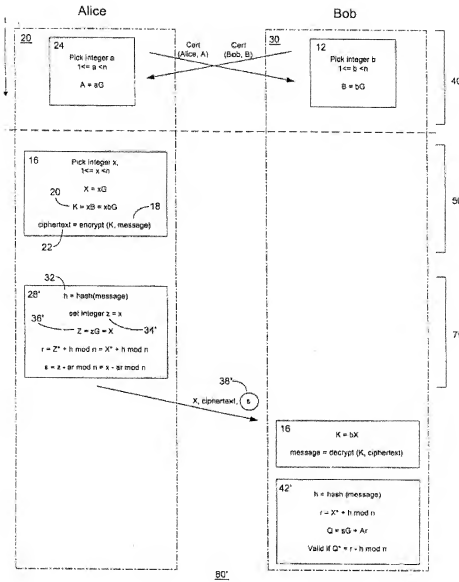

FIG. 4

This "dual use" of an ephemeral key pair in the encryption and digital signature phases of the public key encryption process, and the advantages thereof, is described in the specification as follows:

> "The improved digital signature scheme of the present invention uses the encryption ephemeral key pair (X, x) produced in the encryption stage 50' as a substitute for the signature ephemeral key pair (Z, z) required in the

> digital signature stage 70'. The value of signature ephemeral private key z 34' is set to the value of encryption ephemeral private key x from the encryption stage. Consequently, the random generation of z and the computation of Z 36' are not required since signature ephemeral public key Z 36' equals encryption ephemeral public key X 20. Advantageously, this reduces the computational load on the sender. In essence, the value for x is used for two different purposes. In the first instance, x is used for the encryption process scheme 50'. In the second instance, the x is also used in the digital signature scheme 70'." (Specification, page 9, line 23 through page 10, line 6.)

Based on this explicit disclosure in the specification, applicant maintains that there is adequate support in the application for the dual use of an ephemeral key pair, and thus the section 112 enablement rejection should be withdrawn.

This application is in condition for allowance.

Respectfully submitted:

David B. Cochran

JONES DAY
David B. Cochran
Reg. No. 39,142
901 Lakeside Ave.
Cleveland Ohio, 44114
216-586-7029
dcochran@jonesday.com